

# Substituição de WLAN + VLAN 802.1x com Mobility Express (ME) 8.2 e ISE 2.1

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração em ME](#)

[Declarar-me no ISE](#)

[Criar um novo usuário no ISE](#)

[Criar a regra de autenticação](#)

[Criar a regra de autorização](#)

[Configuração do dispositivo final](#)

[Verificar](#)

[Processo de autenticação em ME](#)

[Processo de autenticação no ISE](#)

## Introduction

Este documento descreve como configurar uma WLAN (Wireless Local Area Network) com segurança empresarial Wi-Fi Protected Access 2 ( WPA2) com um controlador Mobility Express e um servidor Remote Authentication Dial-In User Service (RADIUS). O Identity Service Engine (ISE) é usado como exemplo de servidores RADIUS externos.

O EAP (Extensible Authentication Protocol) usado neste guia é o PEAP (Protected Extensible Authentication Protocol). Além disso, o cliente é atribuído a uma VLAN específica (diferente daquela atribuída ao padrão da WLAN).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- 802,1x
- PEAP
- Autoridade de certificação (CA)
- Certificados

## **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

ME v8.2

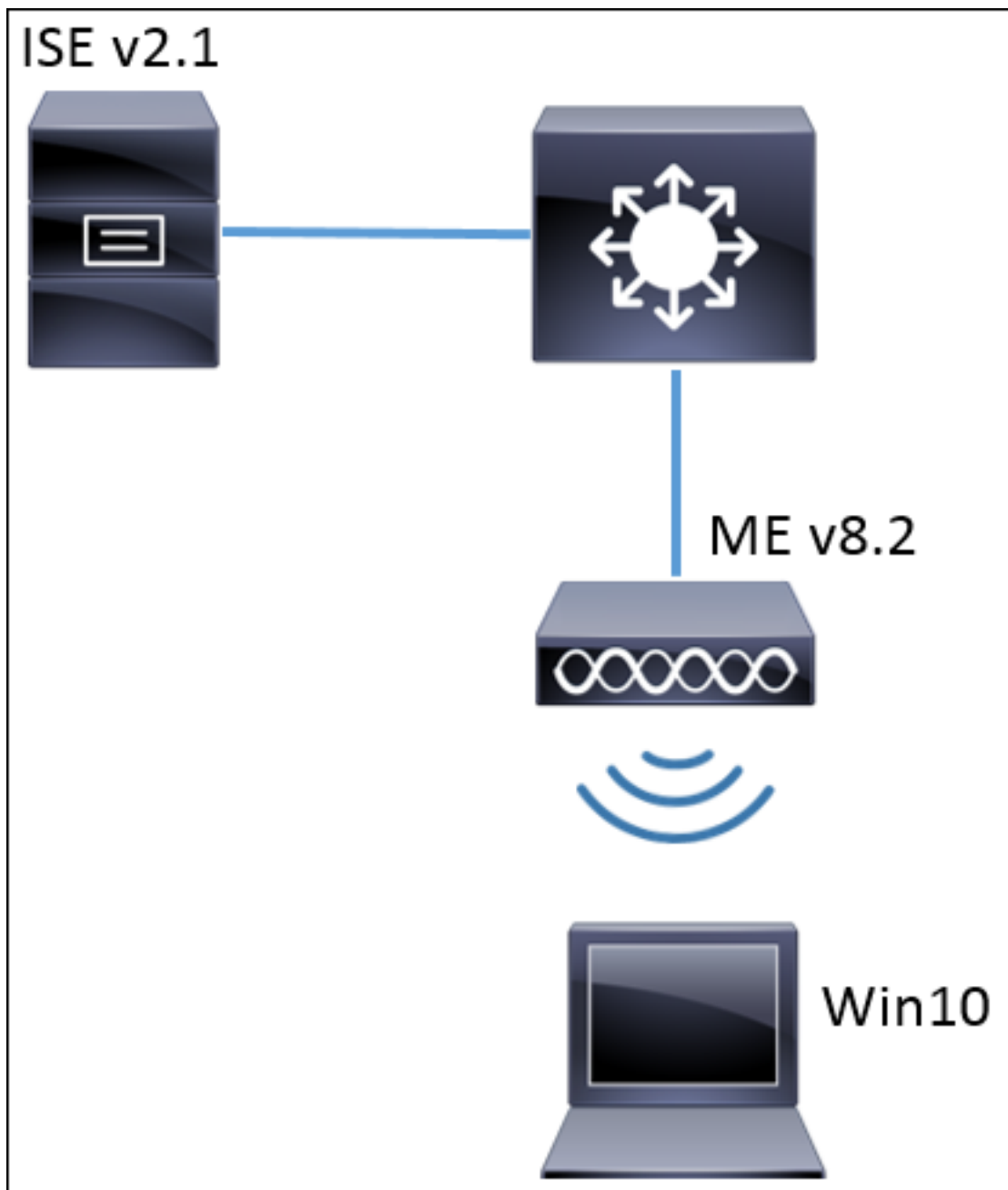
ISE v2.1

Notebook Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## **Configurar**

### **Diagrama de Rede**



### Configurações

As etapas gerais são:

1. Crie o Service Set Identifier (SSID) no ME e declare o servidor RADIUS (ISE neste exemplo) no ME
2. Declarar-me no servidor RADIUS (ISE)
3. Criar a regra de autenticação no ISE
4. Criar a regra de autorização no ISE
5. Configurar o endpoint

### Configuração em ME

Para permitir a comunicação entre o servidor RADIUS e ME, é necessário registrar o servidor RADIUS em ME e vice-versa. Esta etapa mostra como registrar o servidor RADIUS em ME.

Etapa 1. Abra a GUI do ME e navegue até **Configurações sem fio > WLANs > Adicionar nova**

WLAN.

The image shows the Cisco Aironet 1850 S WLAN Configuration interface. On the left, a dark sidebar contains navigation options: Monitoring, Wireless Settings (highlighted with a red box), WLANs (highlighted with a red box), Access Points, WLAN Users, Guest WLANs, Management, and Advanced. The main content area is titled 'WLAN CONFIGURATION' and features a large blue box with a white Wi-Fi icon, the text 'Active WLANs', and a large blue number '2'. At the bottom of the main content area, a button labeled '+ Add new WLAN' is highlighted with a red box.

Etapa 2. Selecione um nome para a WLAN.

## Add New WLAN ✕

General **WLAN Security** VLAN & Firewall QoS

**WLAN Id** 3 ▼

**Profile Name \*** me-ise|

**SSID \*** me-ise

**Admin State** Enabled ▼

**Radio Policy** ALL ▼

✓ Apply ✕ Cancel

Etapa 3. Especifique a configuração de segurança na guia **WLAN Security**.

Escolha **WPA2 Enterprise**, para Servidor de autenticação, escolha **RADIUS externo**. Clique na opção de edição para adicionar o endereço ip do RADIUS e selecionar uma chave **secreta compartilhada**.



# Add New WLAN



General WLAN Security VLAN & Firewall QoS

**Security** WPA2 Enterprise ▼

**Authentication Server** External Radius ▼

	Radius IP ▲	Radius Port	Shared Secret	
		1812	*****	▲
		1812	*****	▼

External Radius configuration applies to all WLANs

Apply

Cancel

Add New WLAN

General WLAN Security VLAN & Firewall QoS

Security WPA2 Enterprise

Authentication Server External Radius

Radius IP ▲ Radius Port Shared Secret

a.b.c.d 1812

Please enter valid IPv4 address

External Radius configuration applies to all WLANs

Apply Cancel

<a.b.c.d> corresponde ao servidor RADIUS.

Etapa 4. Atribua uma VLAN ao SSID.

Se o SSID precisar ser atribuído à VLAN do AP, essa etapa poderá ser ignorada.

Para atribuir os usuários desse SSID a uma VLAN específica (diferente da VLAN do AP), habilite **Usar marcação de VLAN** e atribua o **ID de VLAN** desejado.

The screenshot shows a configuration window titled "Add New WLAN" with a blue header and a close button (X) in the top right corner. Below the header are four tabs: "General", "WLAN Security", "VLAN & Firewall" (which is selected and underlined), and "QoS". The "VLAN & Firewall" tab contains three configuration items, each with a dropdown menu:

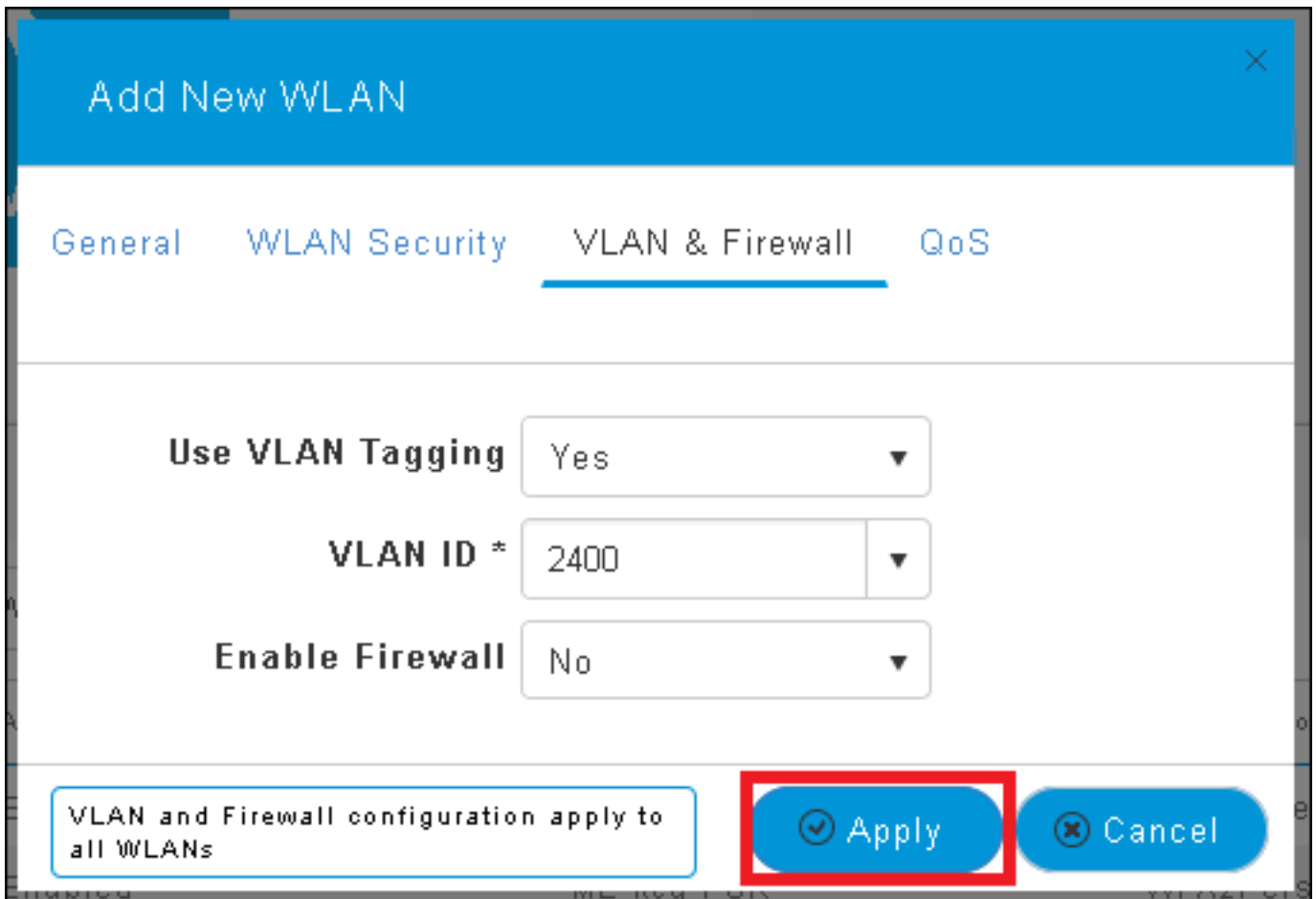
- Use VLAN Tagging**: Set to "Yes".
- VLAN ID \***: Set to "2400".
- Enable Firewall**: Set to "No".

At the bottom of the window, there is a blue-bordered box containing the text: "VLAN and Firewall configuration apply to all WLANs". To the right of this box are two buttons: "Apply" (with a checkmark icon) and "Cancel" (with an X icon).

**Note:** Se a marcação de VLAN for usada, certifique-se de que a porta de switch à qual o ponto de acesso está conectado esteja configurada como porta de tronco e a VLAN do AP esteja configurada como nativa.

Etapa 5. Clique em **Apply** para concluir a configuração.





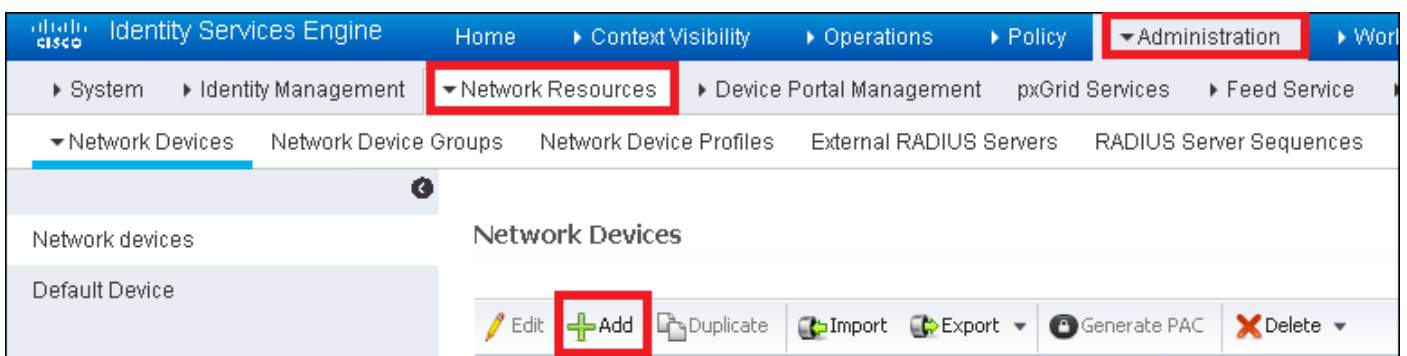
Etapa 6. Opcional, configure a WLAN para aceitar a substituição da VLAN.

Ative a substituição de AAA na WLAN e adicione as VLANs necessárias. Para fazer isso, você precisará abrir uma sessão CLI para a interface de gerenciamento do ME e emitir estes comandos:

```
>config wlan disable <wlan-id>  
>config wlan aaa-override enable <wlan-id>  
>config wlan enable <wlan-id>  
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

#### Declarar-me no ISE

Etapa 1. Abra o console do ISE e navegue até **Administration > Network Resources > Network Devices > Add**.



Etapa 2. Inserir informações.

Opcionalmente, ele pode ser especificado como Nome do modelo, versão do software, descrição e atribuição de grupos de dispositivos de rede com base em tipos de dispositivos, localização ou WLCs.

a.b.c.d corresponde ao endereço IP do ME.

Network Devices List > **New Network Device**

### Network Devices

\* Name

Description

\* IP Address:  /

\* Device Profile  Cisco

Model Name

Software Version

\* Network Device Group

Device Type

Location

WLCs

**▼ RADIUS Authentication Settings**

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

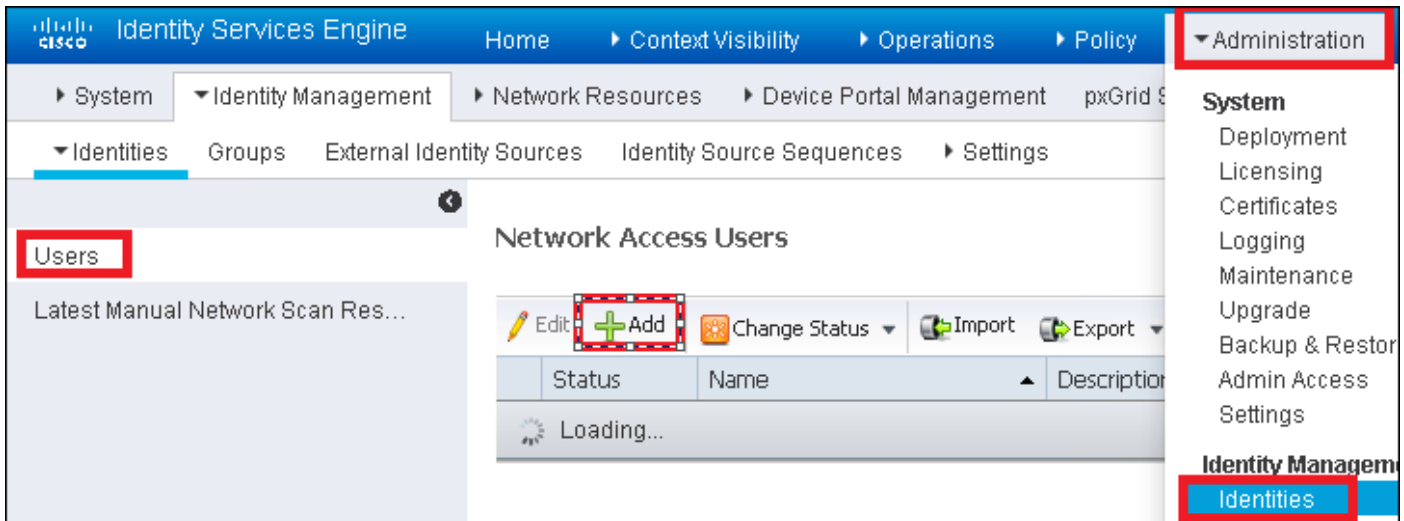
CoA Port

Para obter mais informações sobre Grupos de dispositivos de rede, consulte este link:

[ISE - Grupos de dispositivos de rede](#)

Criar um novo usuário no ISE

Etapa 1. Navegar para **Administração > Gerenciamento de Identidades > Identidades > Usuários > Adicionar**.



Etapa 2. Inserir informações.

Neste exemplo, este usuário pertence a um grupo chamado ALL\_ACCOUNTS, mas pode ser ajustado conforme necessário.

▼ Network Access User

\* Name

Status  Enabled ▼

Email

▼ Passwords

Password Type:  ▼

Password

Re-Enter Passw

\* Login Password

Enable Password

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ Account Disable Policy

Disable account if date exceeds

▼ User Groups

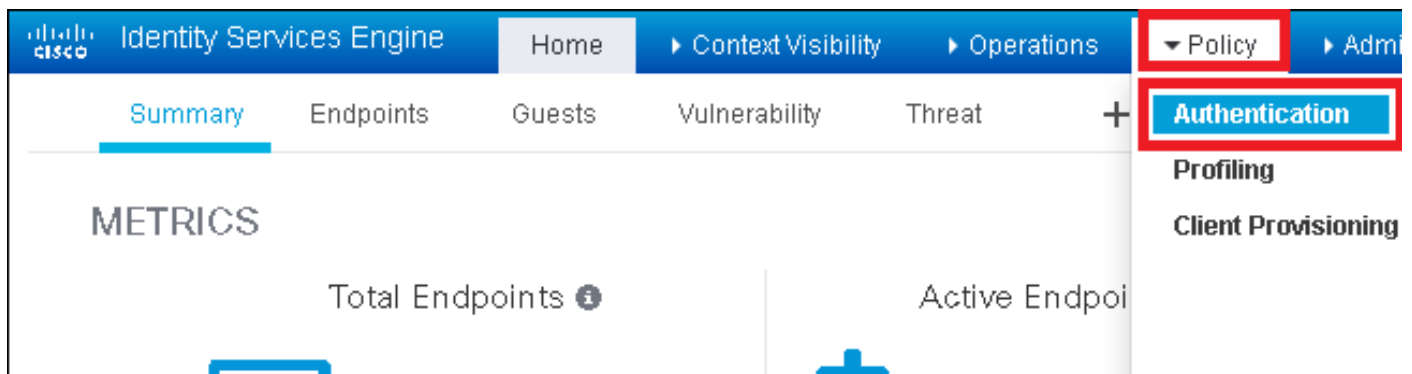
+

Criar a regra de autenticação

As regras de autenticação são usadas para verificar se as credenciais dos usuários estão corretas (verifique se o usuário realmente é quem ele diz ser) e limite os métodos de autenticação

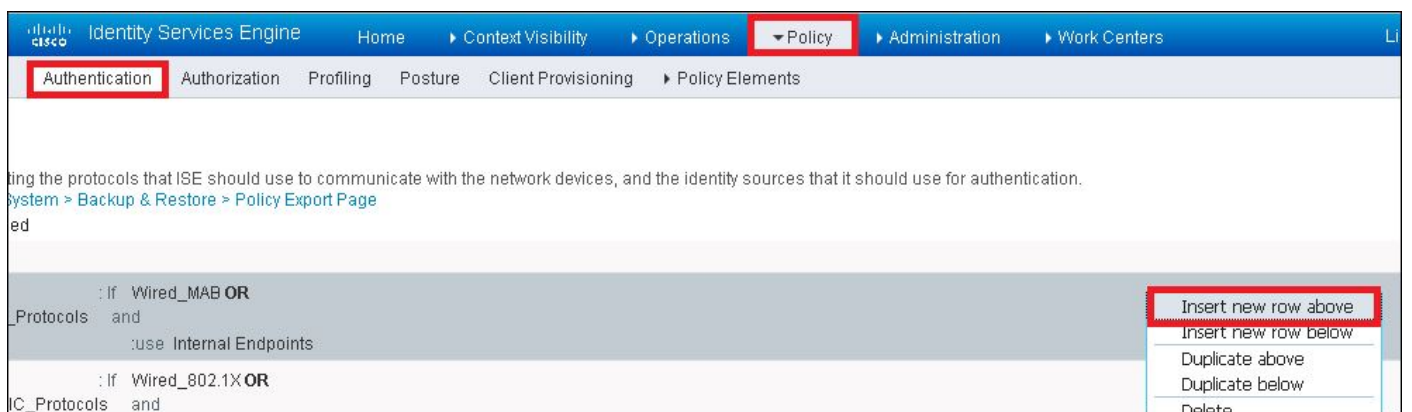
que podem ser usados por ele.

Etapa 1. Navegar para **Política > Autenticação**.



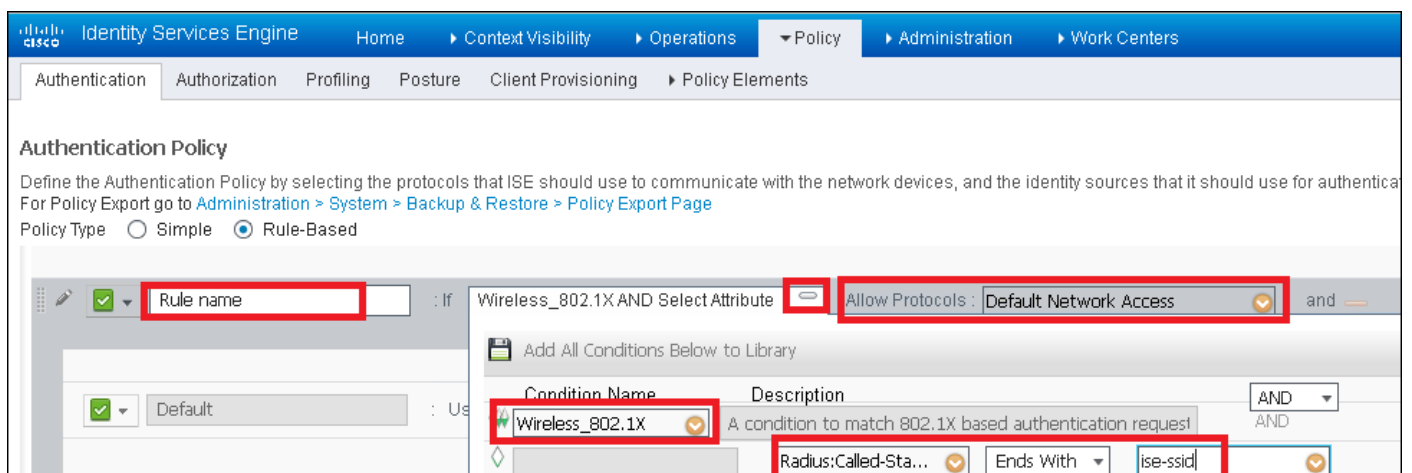
Etapa 2. Insira uma nova regra de autenticação.

Para fazer isso, navegue para **Política > Autenticação > Inserir nova linha acima/abaixo**.

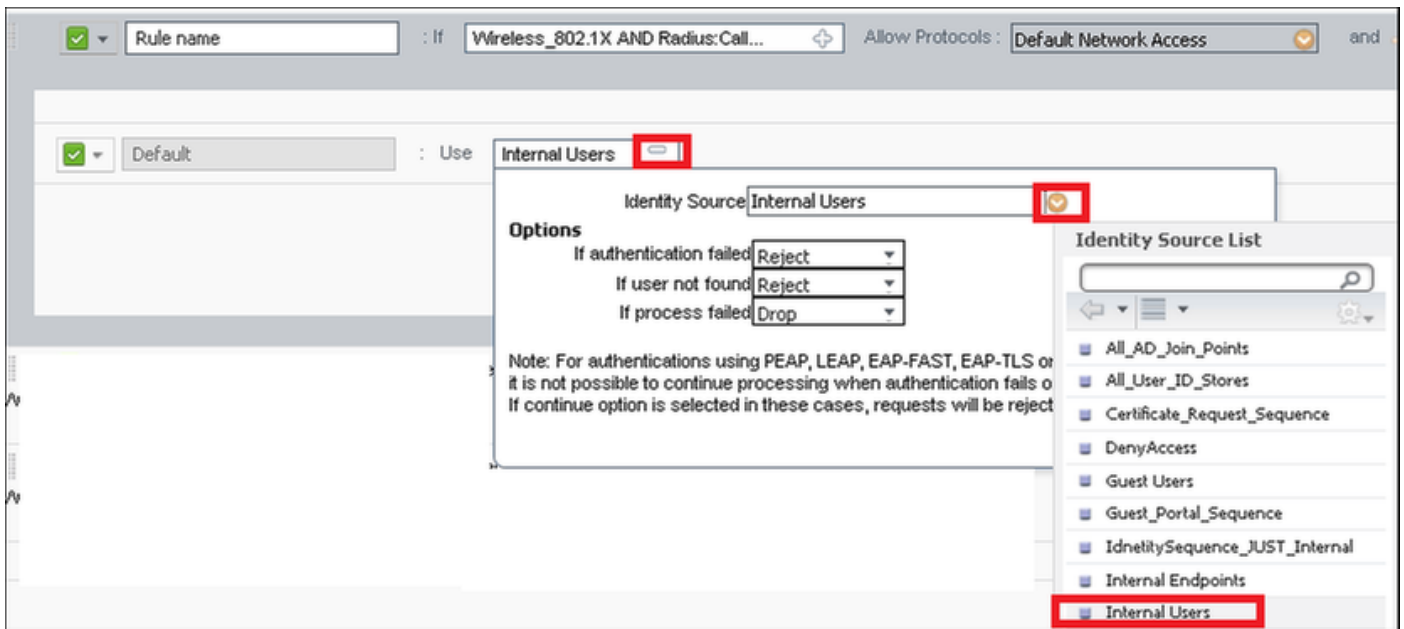


Etapa 3. Insira as informações necessárias

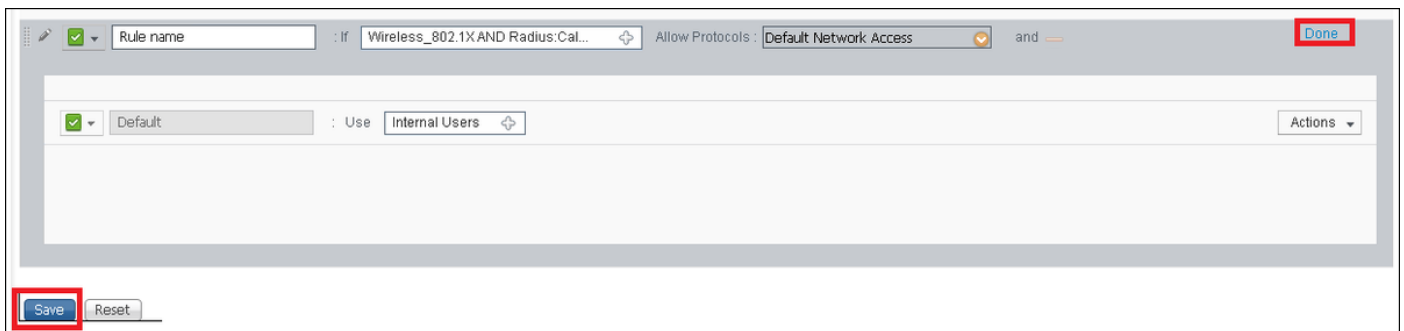
Este exemplo de regra de autenticação permite todos os protocolos listados na lista **Acesso de Rede Padrão**, que se aplica à solicitação de autenticação para clientes Wireless 802.1x e com ID de Estação Chamada e termina com *ise-ssid*.



Além disso, escolha a origem da identidade para os clientes que correspondem a esta regra de autenticação, neste exemplo ela é usada *por usuários internos*



Depois de concluir, clique em **Concluído e Salvar**



Para obter mais informações sobre Permitir Políticas de Protocolos, consulte este link:

[Serviço de Protocolos Permitidos](#)

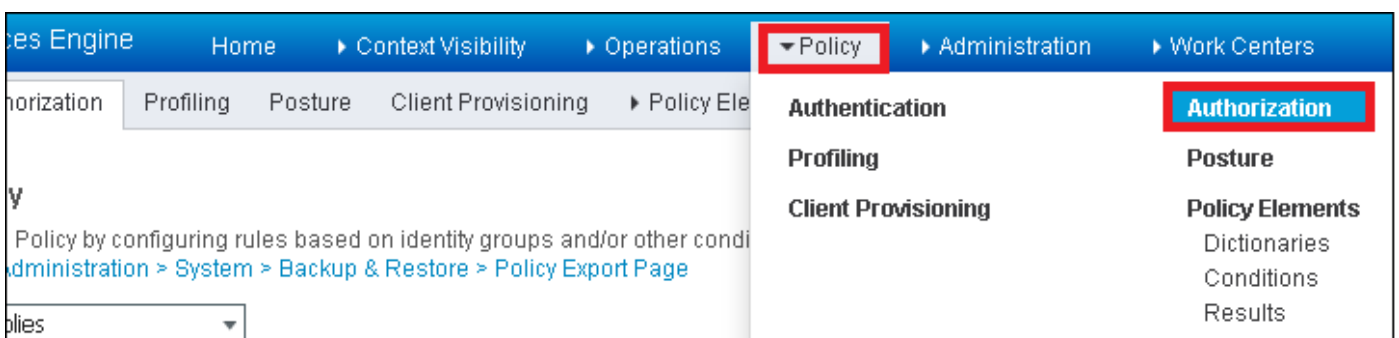
Para obter mais informações sobre fontes de identidade, consulte este link:

[Criar um grupo de identidade de usuário](#)

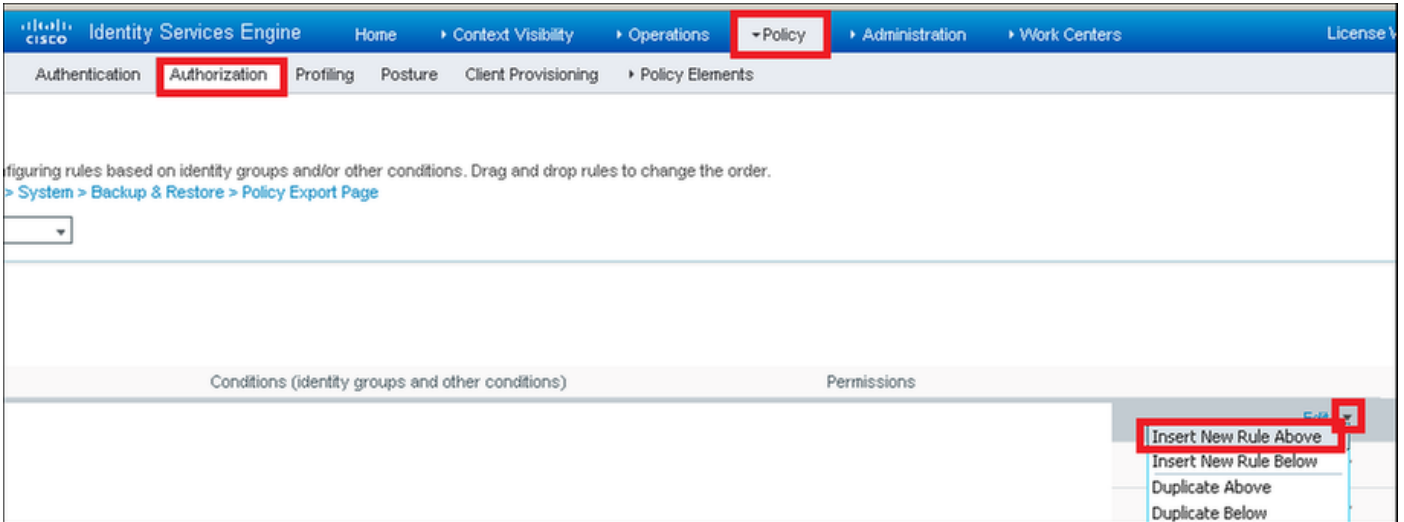
### Criar a regra de autorização

A regra de autorização é a responsável para determinar se o cliente pode ou não ingressar na rede

Etapa 1. Navegue até **Política > Autorização**.

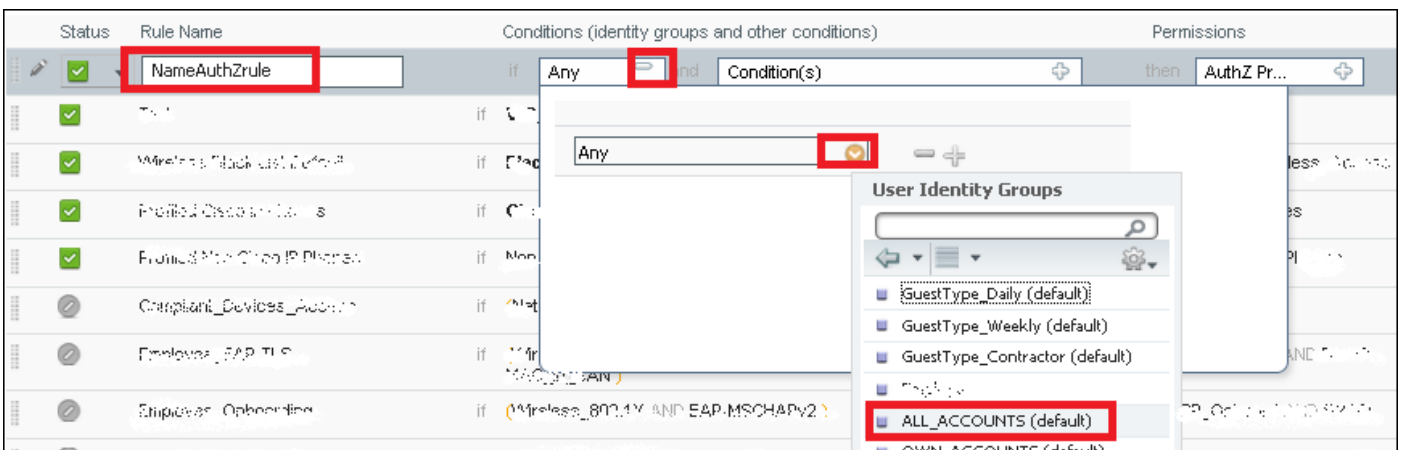


Etapa 2. Inserir uma nova regra. Navegue até **Política > Autorização > Inserir nova regra acima/abaixo**.

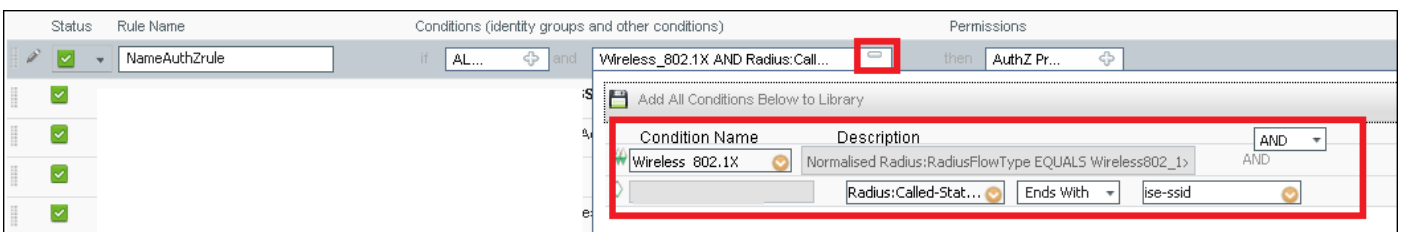


Etapa 3. Inserir informações.

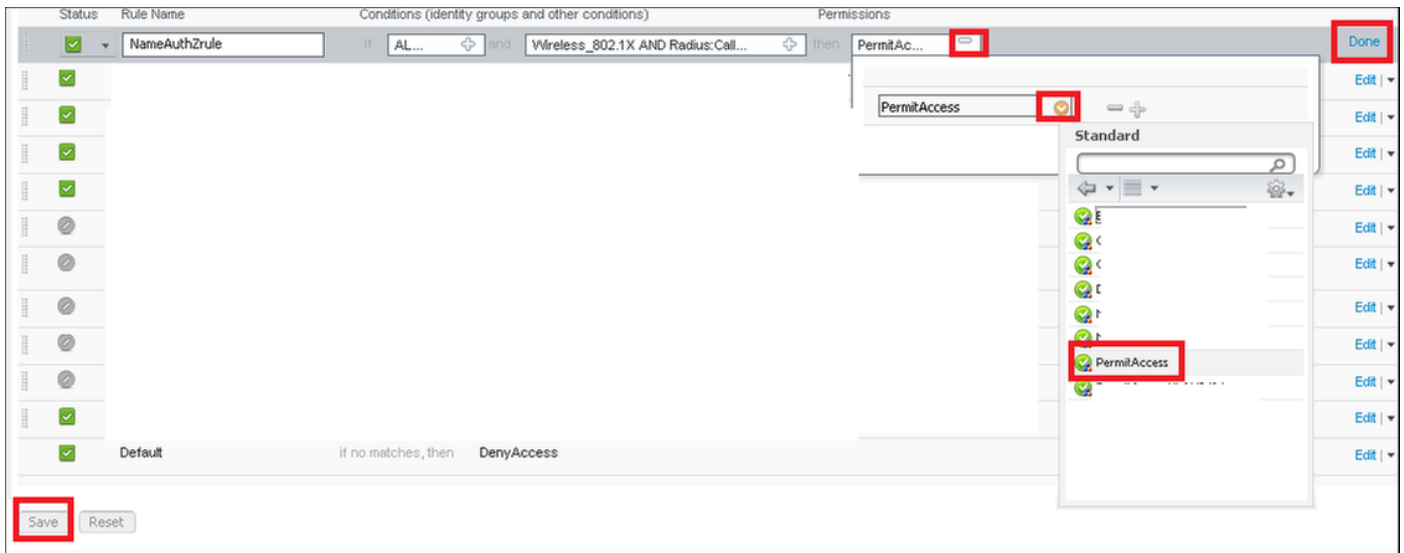
Primeiro escolha um nome para a regra e os grupos de identidades onde o usuário está armazenado. Neste exemplo, o usuário é armazenado no grupo **ALL\_ACCOUNTS**.



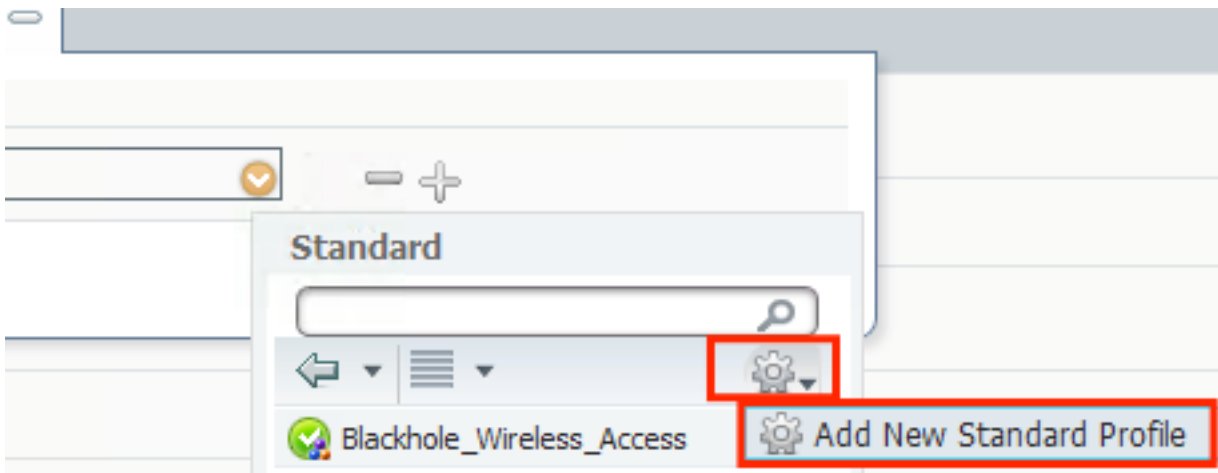
Depois disso, escolha outras condições que façam com que o processo de autorização se enquadre nessa regra. Neste exemplo, o processo de autorização atinge esta regra se ela usa 802.1x Wireless e é chamada de ID da estação termina com *ise-ssid*.



Finalmente, escolha o perfil de autorização que permite que os clientes ingressem na rede, clique em **Concluído e Salvar**.



Opcionalmente, crie um novo perfil de autorização que atribua o cliente sem fio a uma VLAN diferente:



Inserir informações:



Add New Standard Profile

**Authorization Profile**

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

**Common Tasks**

DACL Name

ACL (Filter-ID)

VLAN Tag ID   IDName

Voice Domain Permission

**Advanced Attributes Settings**

Select an item =  +

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
Tunnel-Private-Group-ID = 1:vlan-id  
Tunnel-Type = 1:13  
Tunnel-Medium-Type = 1:6

## Configuração do dispositivo final

Configurar um computador portátil Windows 10 para ligar a um SSID com autenticação 802.1x utilizando PEAP/MS-CHAPv2 (versão Microsoft do Challenge-Handshake Authentication Protocol versão 2).

Neste exemplo de configuração, o ISE usa seu certificado autoassinado para executar a autenticação.

Para criar o perfil da WLAN na máquina Windows, há duas opções:

1. Instalar o certificado autoassinado na máquina para validar e confiar no servidor ISE para concluir a autenticação
2. Ignorar a validação do servidor RADIUS e confiar em qualquer servidor RADIUS usado para executar a autenticação (não recomendado, pois pode se tornar um problema de segurança)

A configuração dessas opções é explicada na [configuração do dispositivo final - Create the WLAN Profile - Step 7](#).

## Configuração do dispositivo final - Instalar certificado autoassinado do ISE

Etapa 1. Exportar certificado autoassinado do ISE.

Faça login no ISE e navegue até **Administration > System > Certificados > System Certificados**.

Em seguida, selecione o certificado usado para a **autenticação EAP** e clique em **Exportar**.

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation path is: System > Certificates > System Certificates. The 'Export' button is highlighted. Below the buttons is a table of certificates:

	Friendly Name	Used By	Portal group tag
<input checked="" type="checkbox"/>	EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#000001	EAP Authentication	

Salve o certificado no local necessário. Este certificado está instalado na máquina do Windows.

The dialog box is titled "Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#000001'". It contains the following options:

- Export Certificate Only
- Export Certificate and Private Key

There are two input fields:

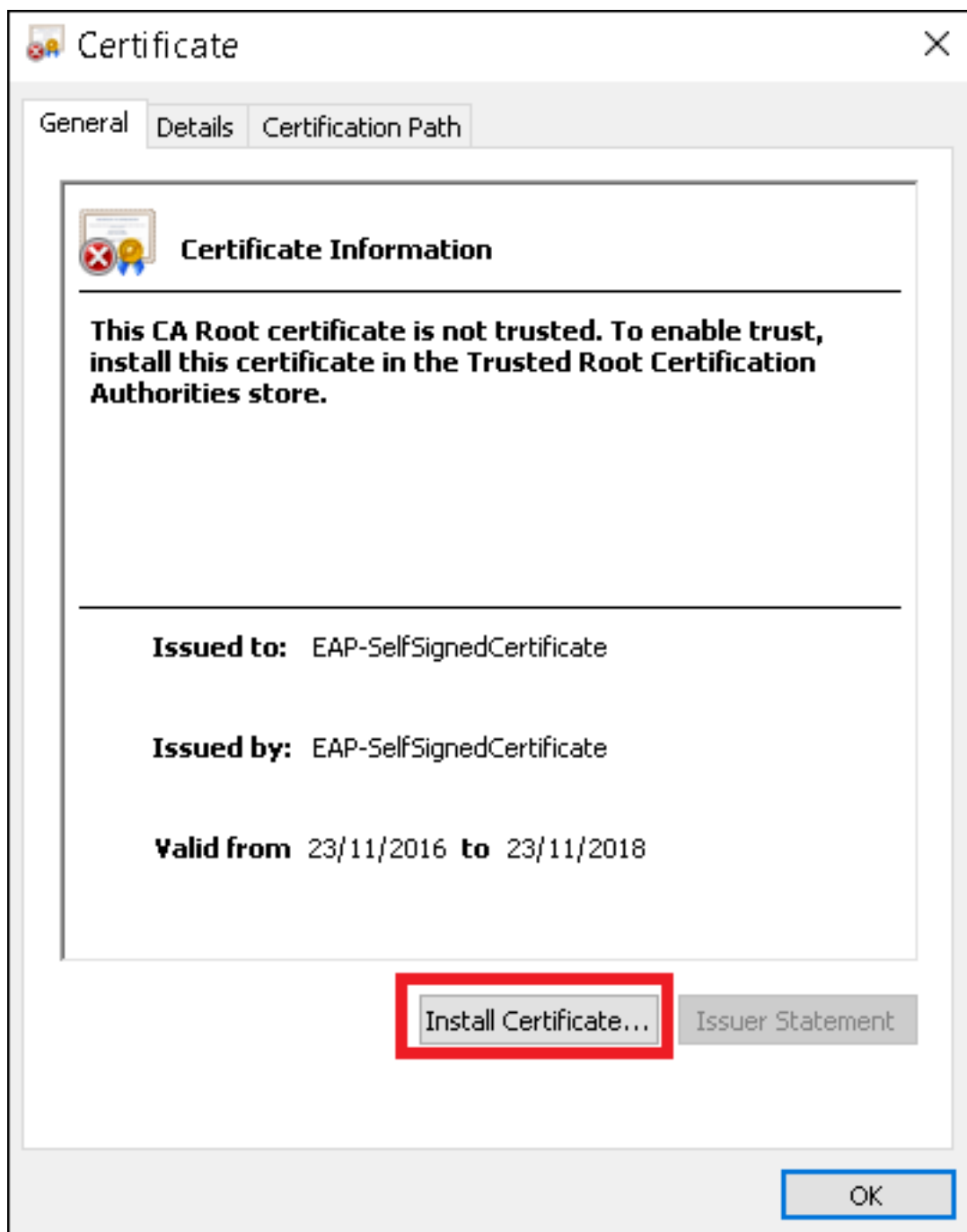
- \*Private Key Password
- \*Confirm Password

A warning message is displayed: **Warning:** Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

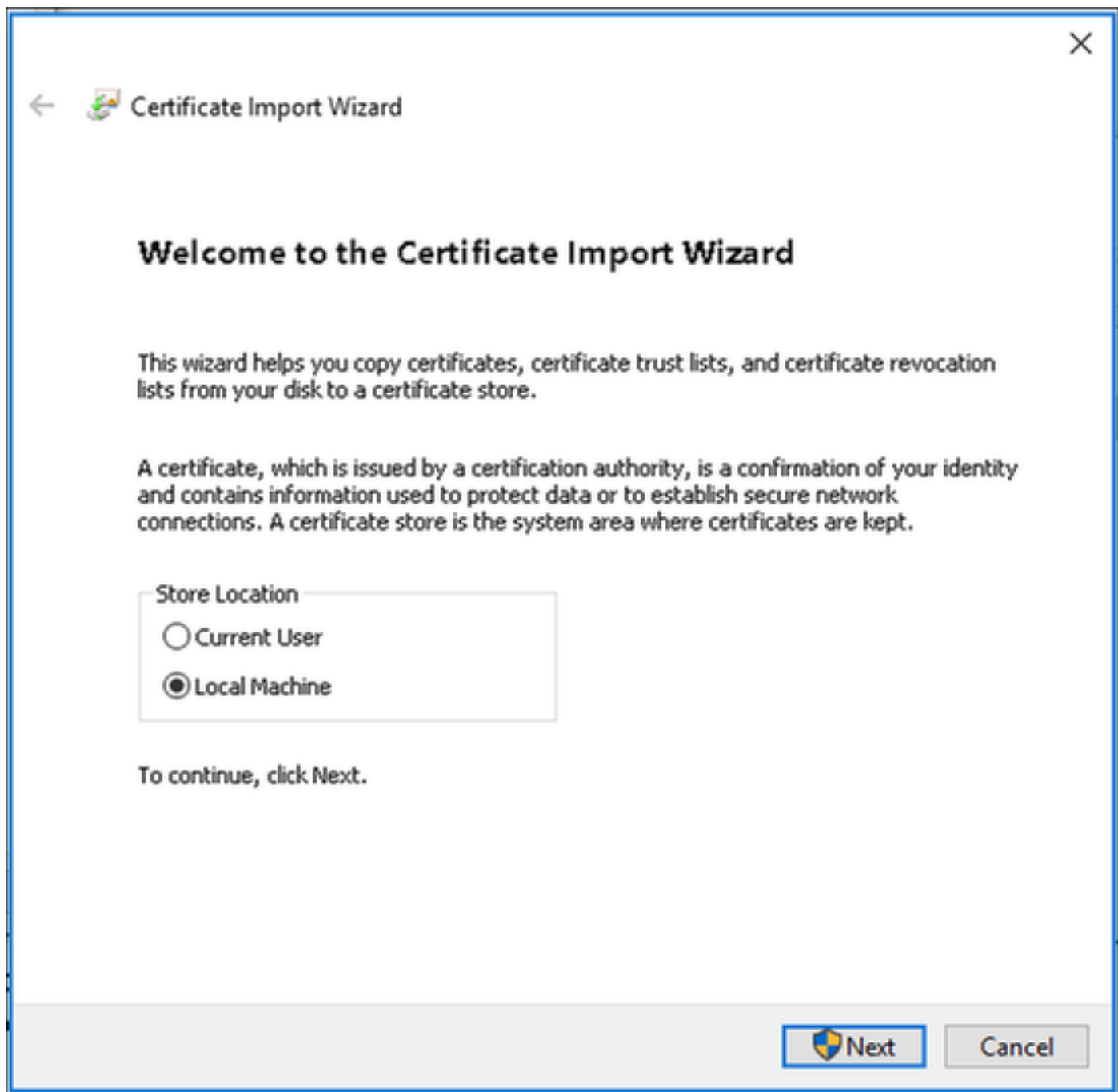
The "Export" button is highlighted.

Etapa 2. Instale o certificado na máquina do Windows.

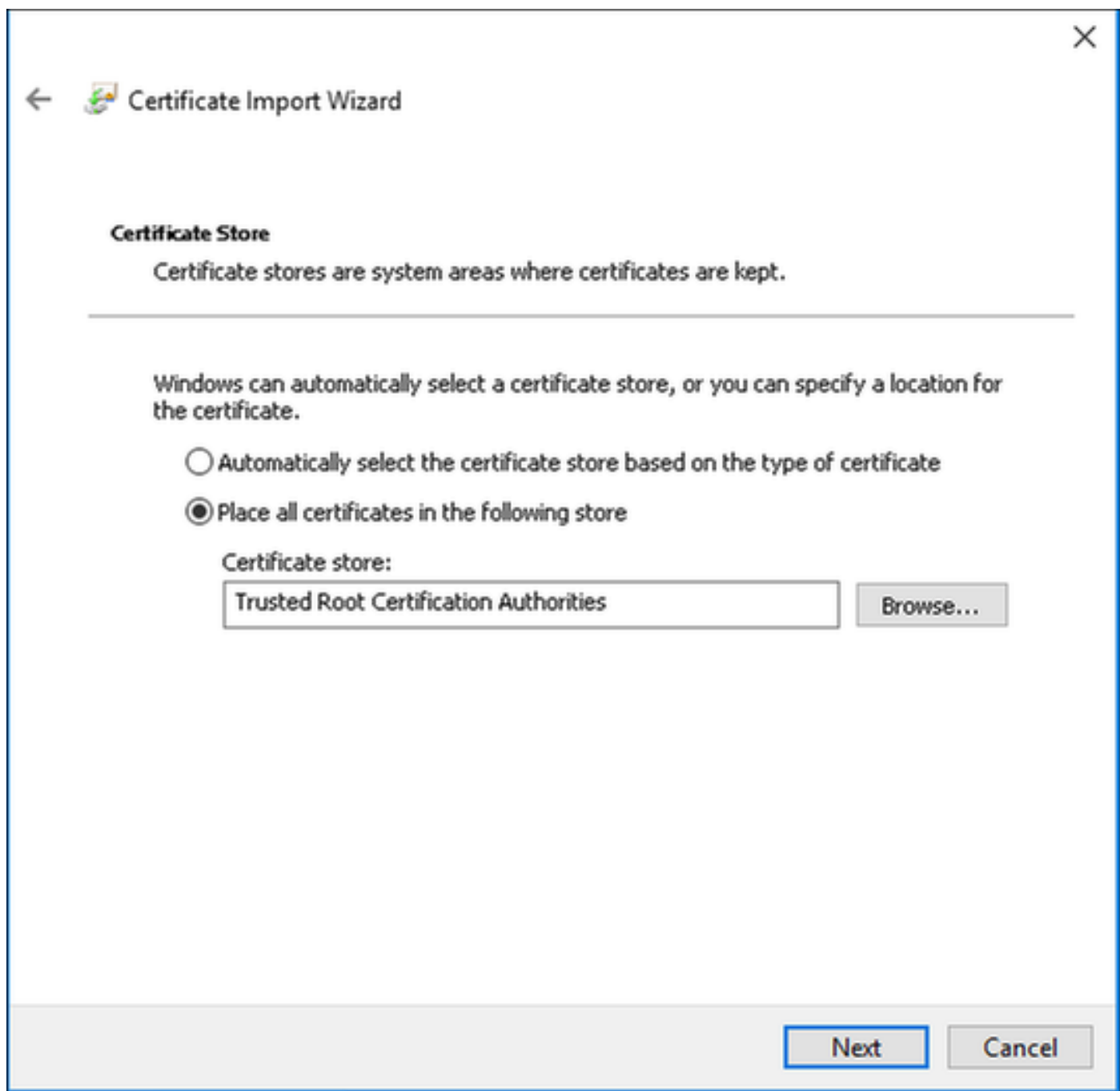
Copie o certificado exportado antes para a máquina do Windows, altere a extensão do arquivo de .pem para .crt, depois de clicar duas vezes nele e selecione **Instalar certificado...**



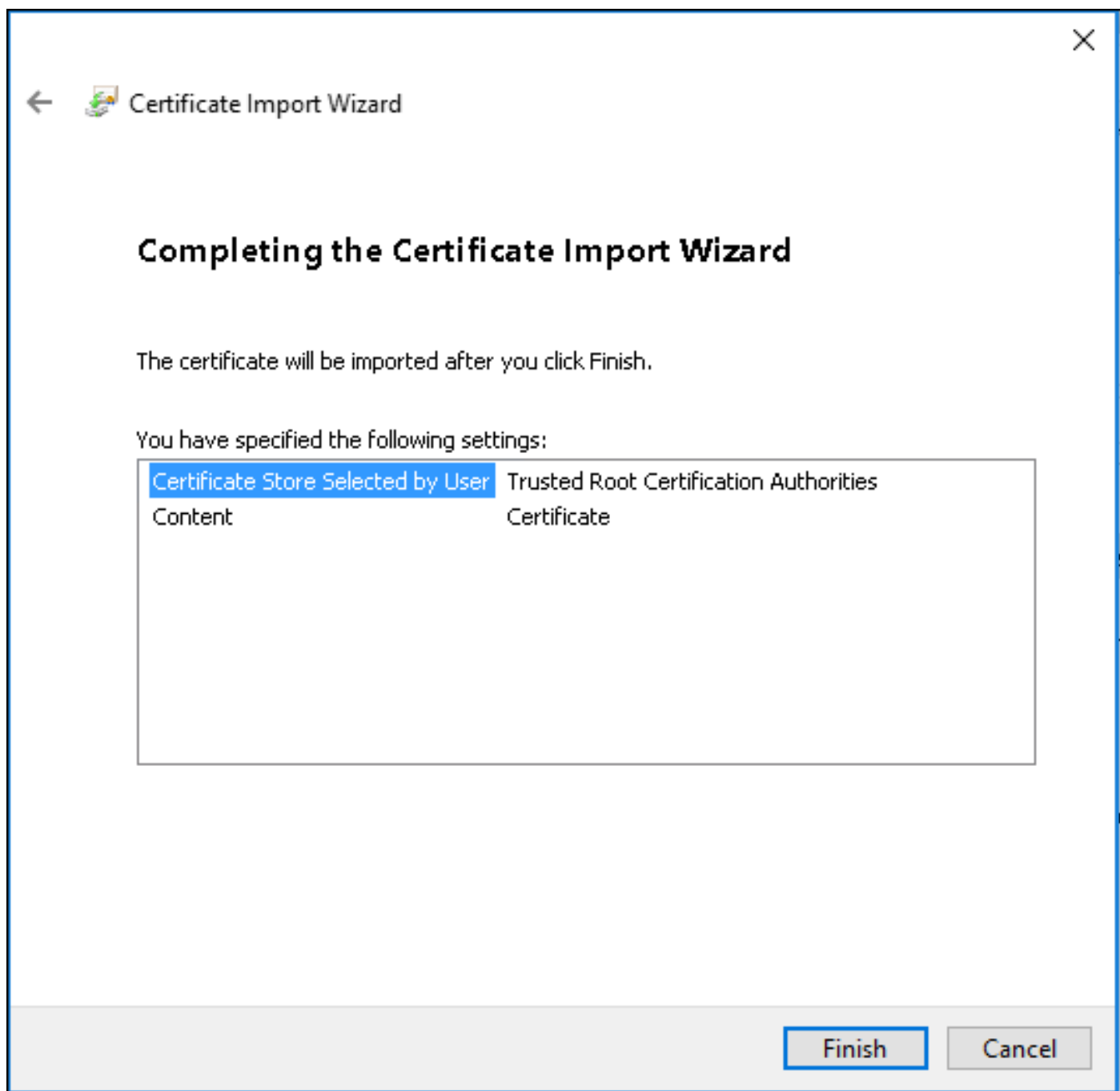
Escolha instalá-lo na **máquina local** e clique em **Avançar**.



Selecione **Colocar todos os certificados na loja a seguir** e, em seguida, navegue e escolha **Autoridades de Certificação de Raiz Confiáveis**. Depois disso, clique em **Avançar**.



Em seguida, clique em **Concluir**.



No final, clique em **Sim** para confirmar a instalação do certificado.

## Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): 011A193D 7007713D 0204E3D0 4759215D  
4294213C

### Warning:

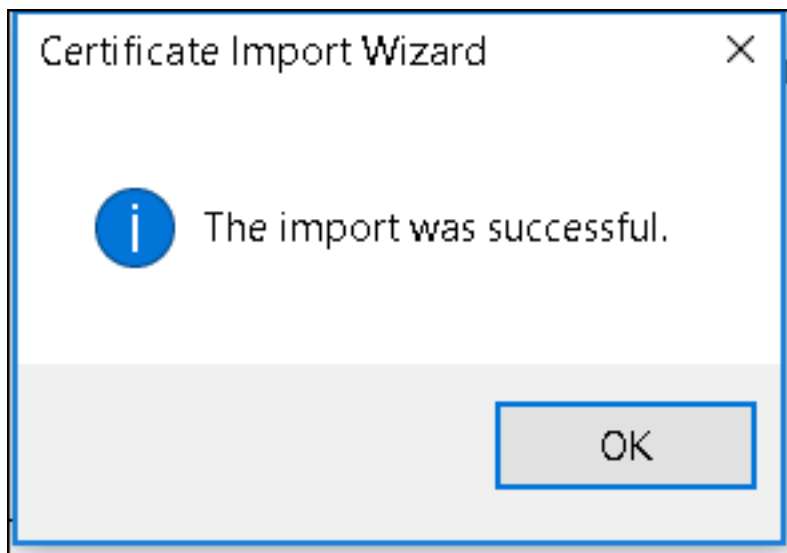
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes

No

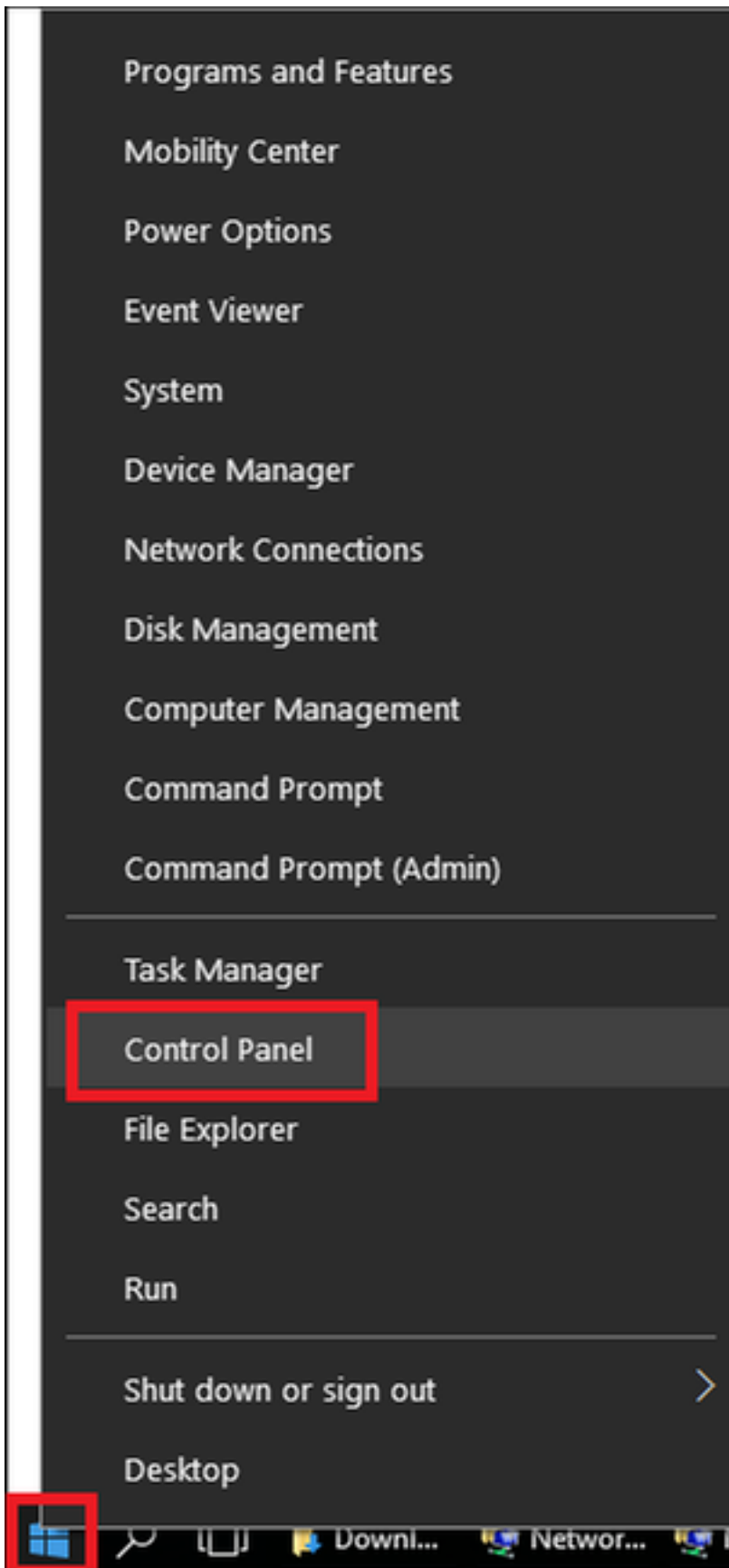
Finalmente, clique em **OK**.



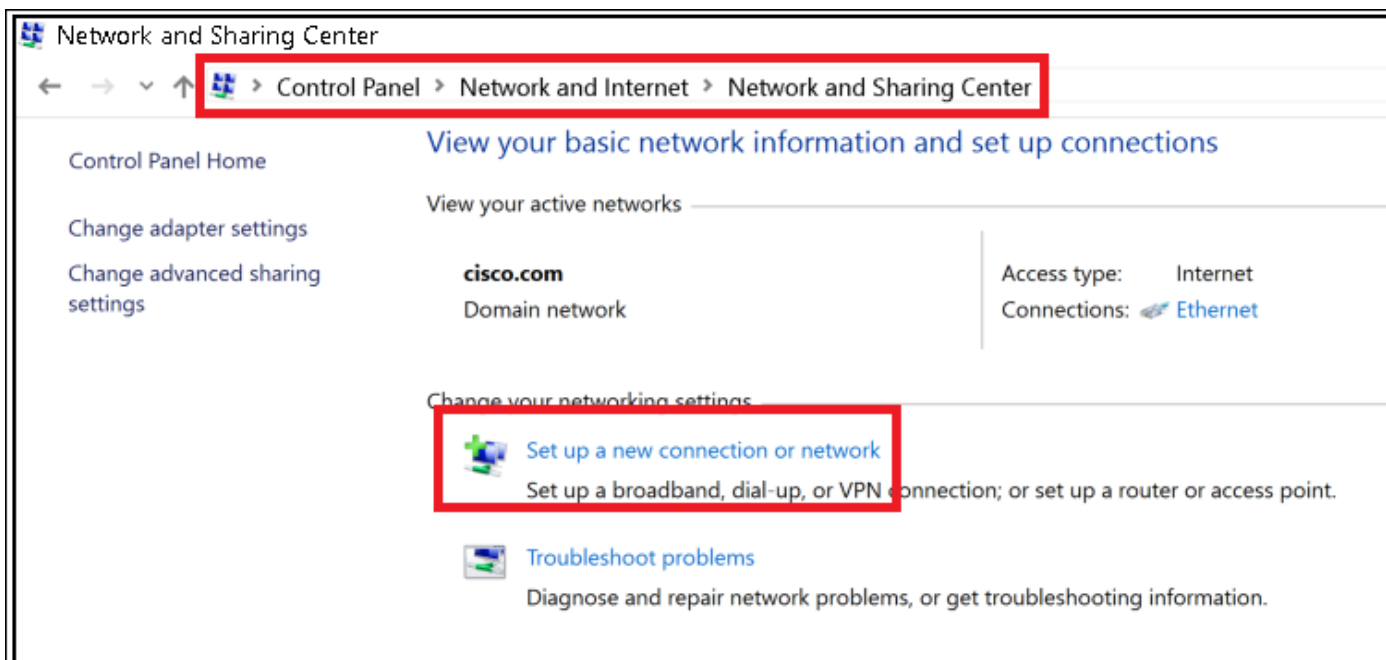
Configuração do dispositivo final - Criar o perfil da WLAN

Etapa 1. Clique com o botão direito do mouse no ícone **Iniciar** e selecione **Painel de controle**.

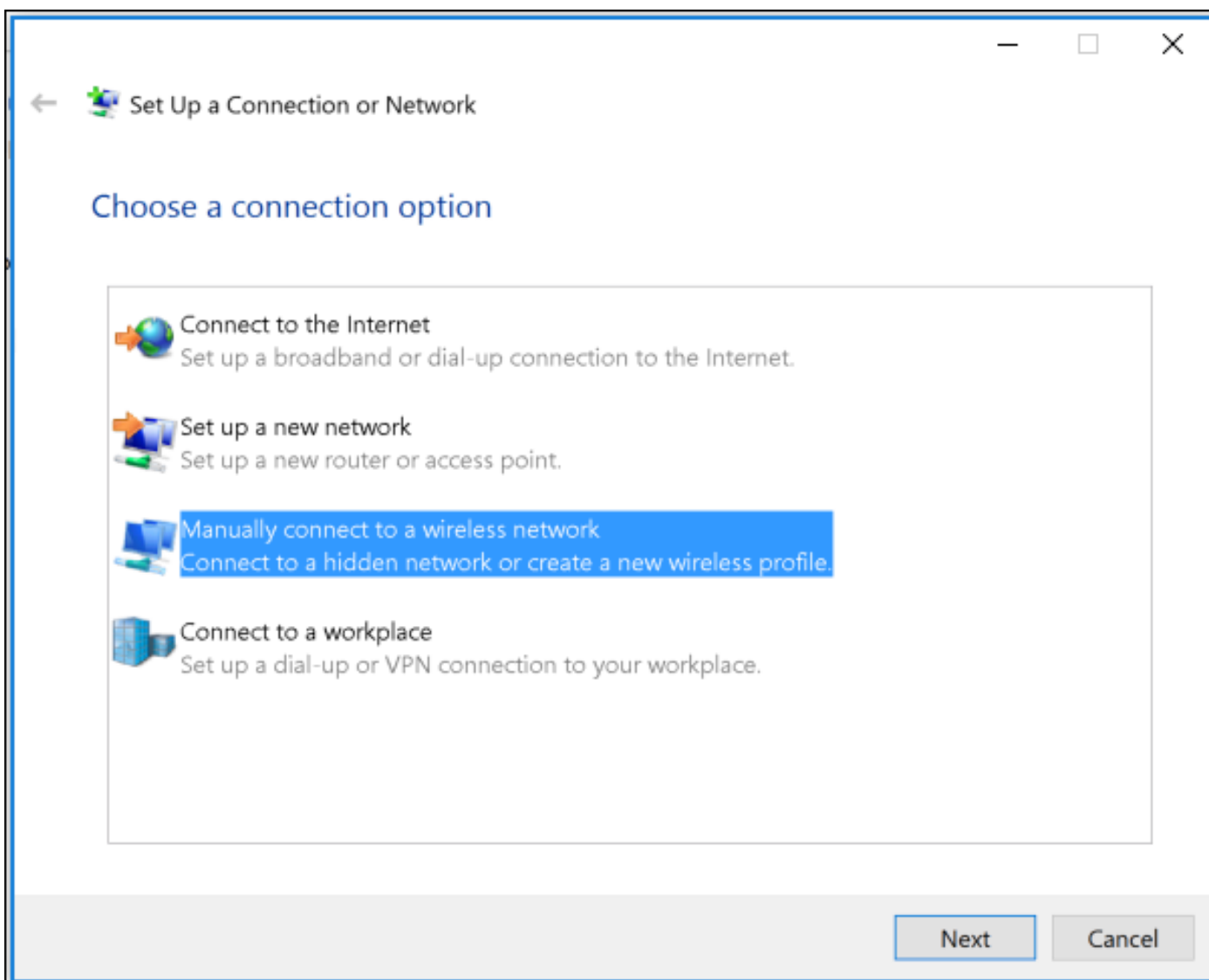




Etapa 2. Navegue até **Rede e Internet** e, em seguida, para **Central de Rede e Compartilhamento** e clique em **Configurar uma nova conexão ou rede**.



Etapa 3. Selecione **Conectar manualmente a uma rede sem fio** e clique em **Avançar**.



Etapa 4. Insira as informações com o nome do SSID e o tipo de segurança WPA2-Enterprise e clique em **Avançar**.

← Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

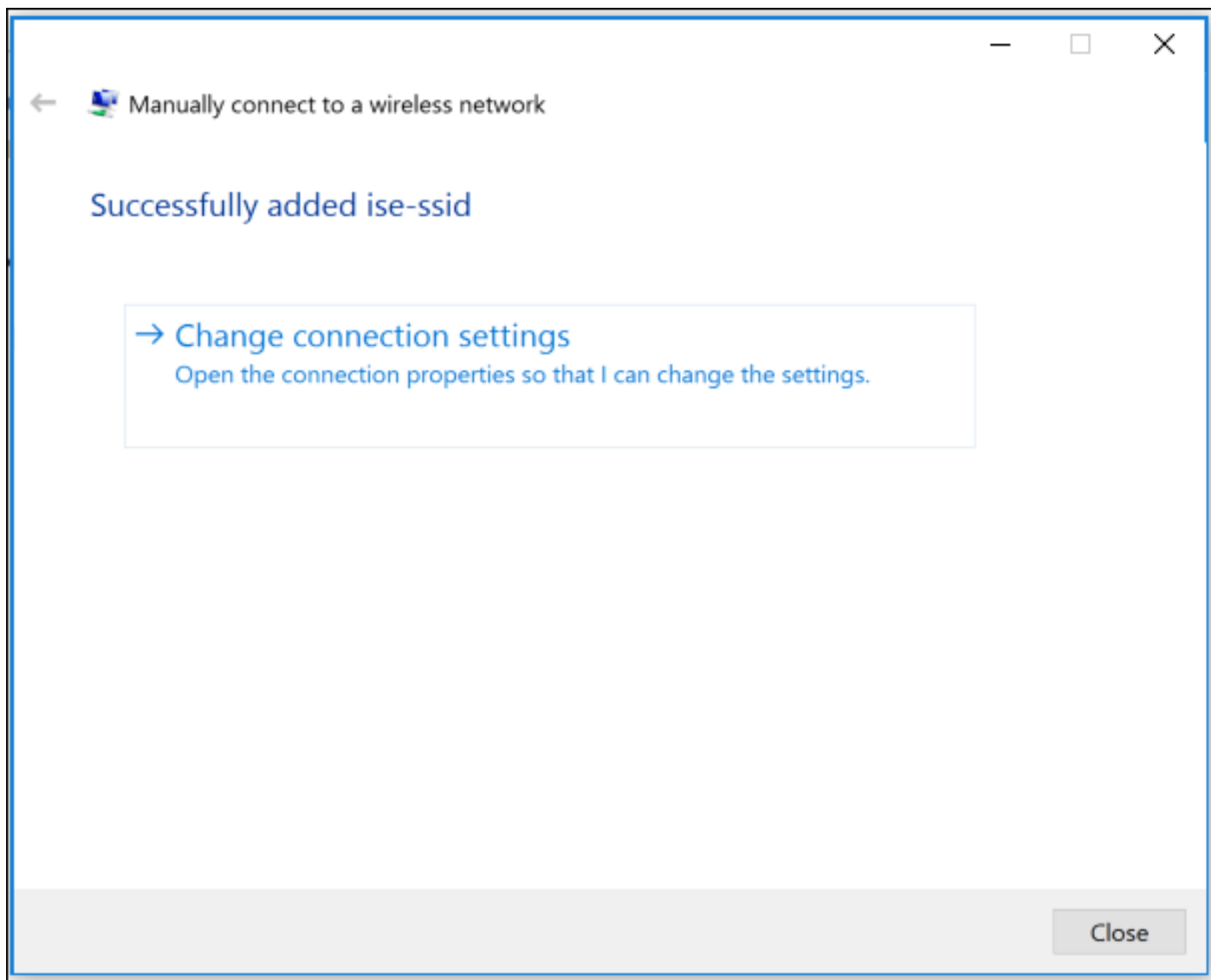
Security Key:   Hide characters

Start this connection automatically

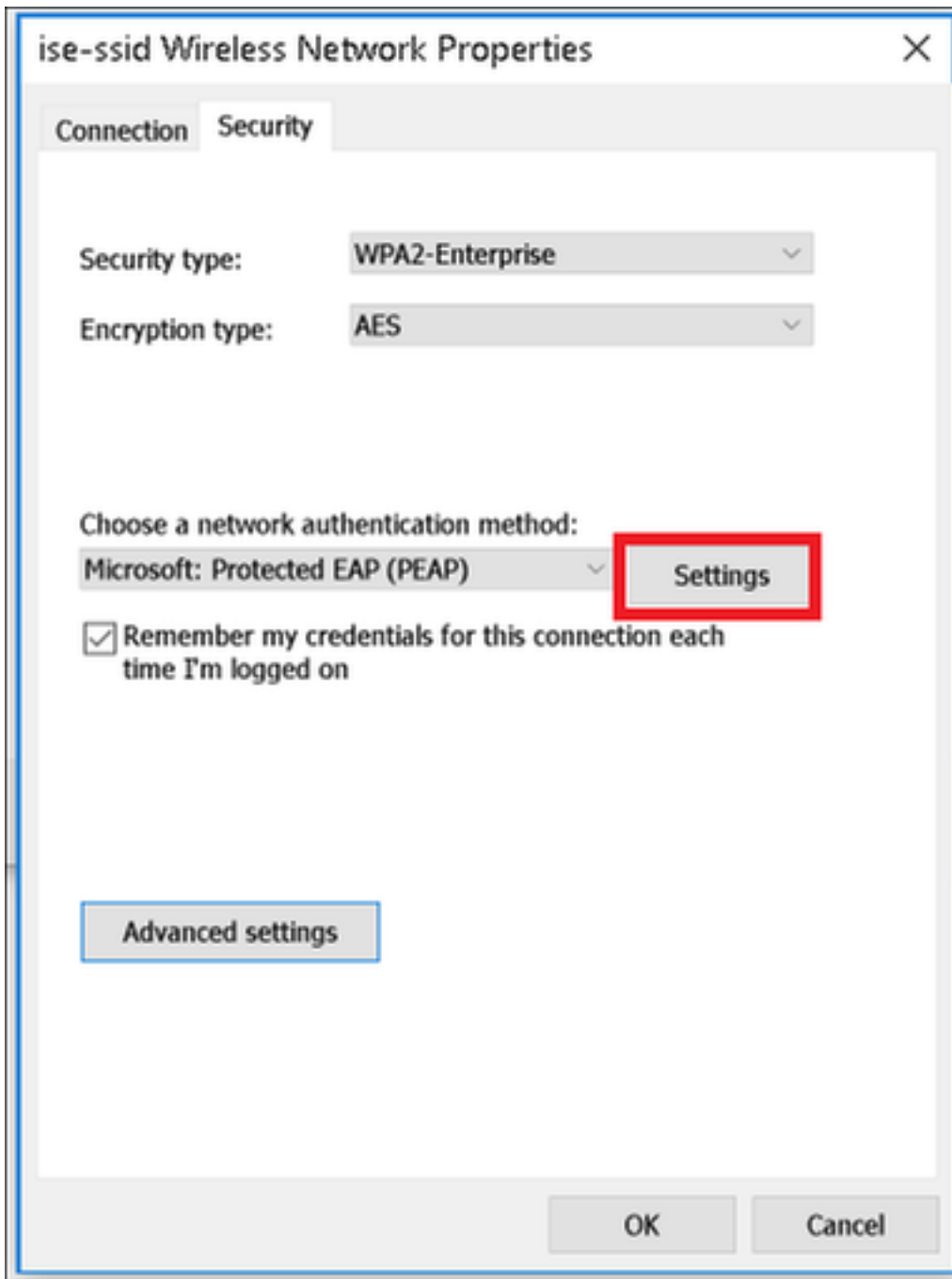
Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Etapa 5. Selecione **Alterar configurações de conexão** para personalizar a configuração do perfil da WLAN.



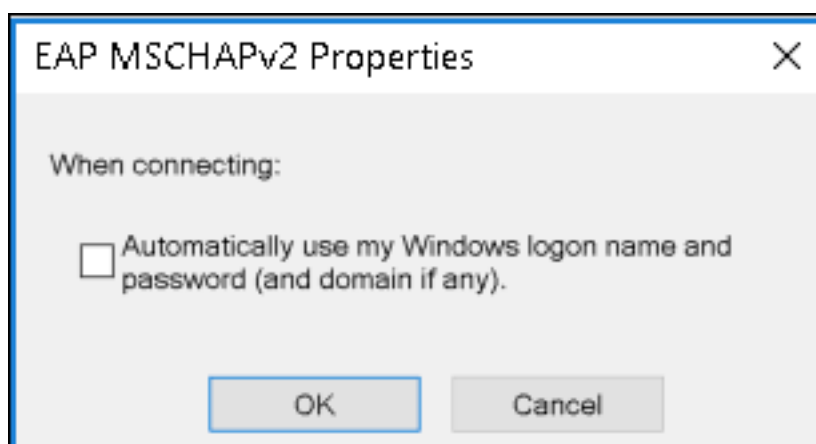
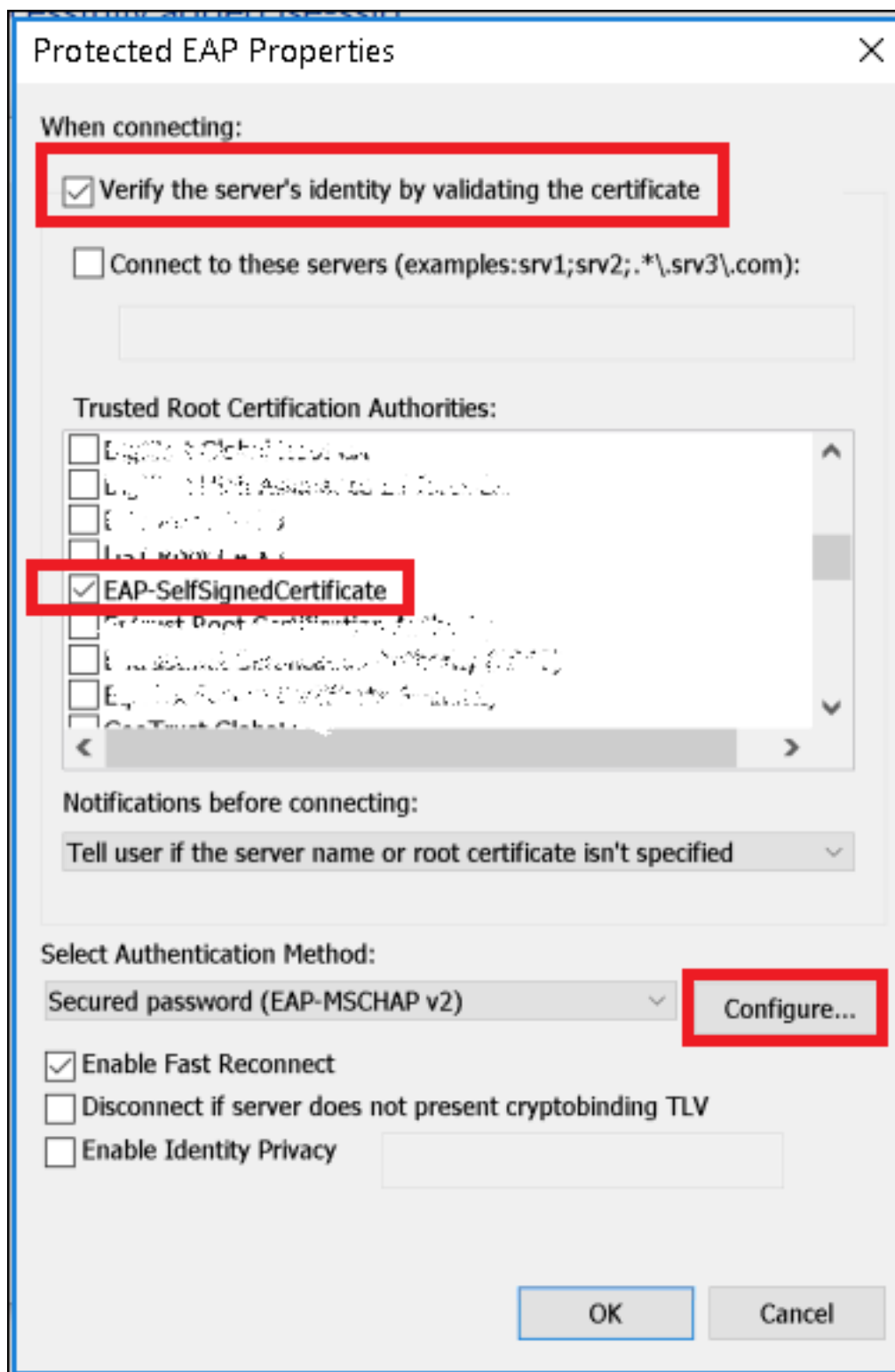
Etapa 6. Navegue até a guia **Segurança** e clique em **Configurações**.



Passo 7. Escolha se o servidor RADIUS é validado ou não.

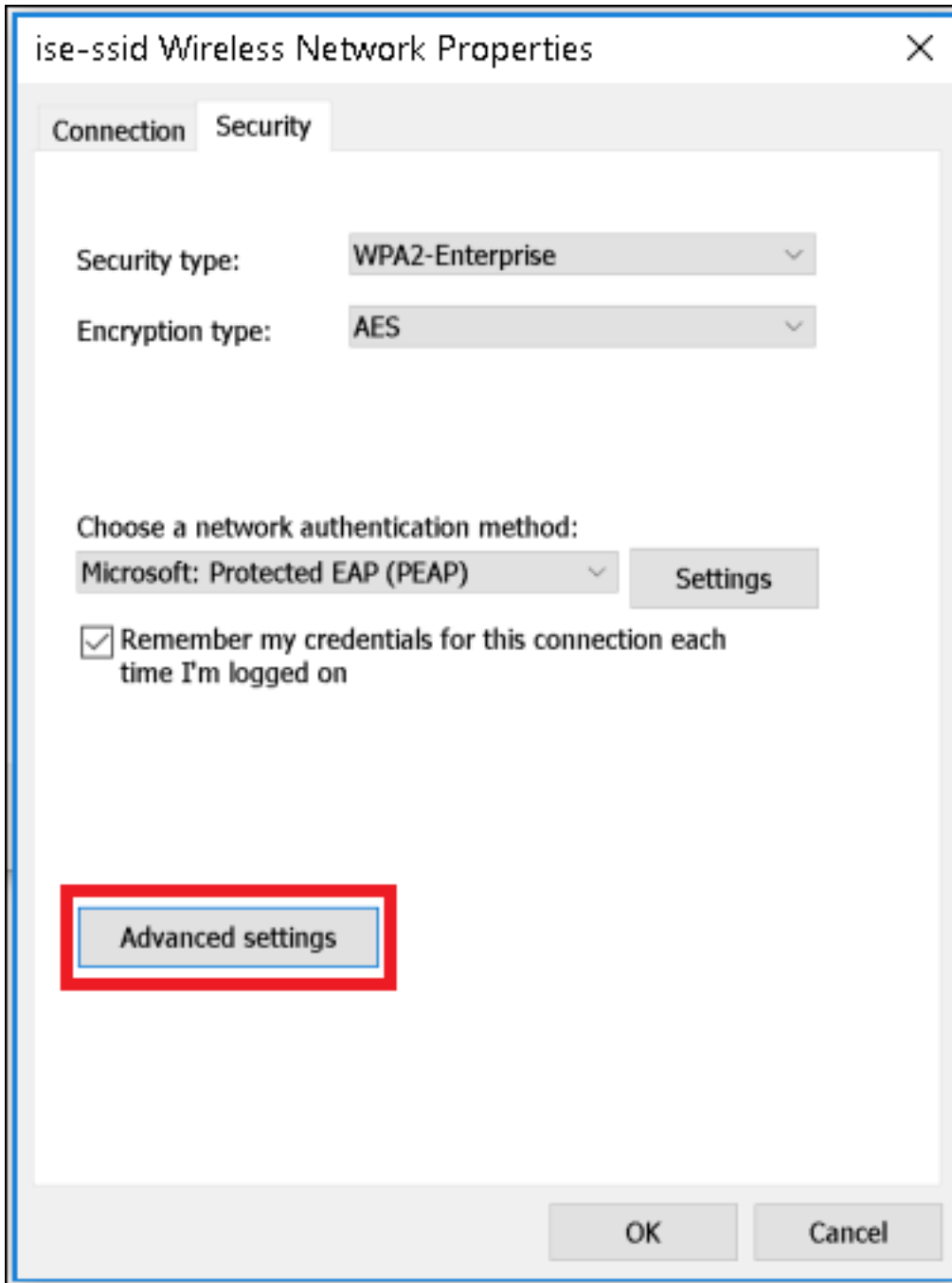
Em caso afirmativo, habilite **Verifique a identidade do servidor validando o certificado** e na **Lista de autoridades de certificação raiz confiáveis**: selecione o certificado autoassinado do ISE.

Depois disso, selecione **Configurar** e desative **Utilizar automaticamente o nome de início de sessão e a senha do Windows...** e, em seguida, clique em **OK**



## Etapa 8. Configurar as credenciais do usuário

Depois de voltar à guia **Segurança**, selecione **Configurações avançadas**, especifique o modo de autenticação como **autenticação do usuário** e salve as credenciais configuradas no ISE para autenticar o usuário.



## Advanced settings



802.1X settings

802.11 settings

Specify authentication mode:

User authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

Maximum delay (seconds):

10

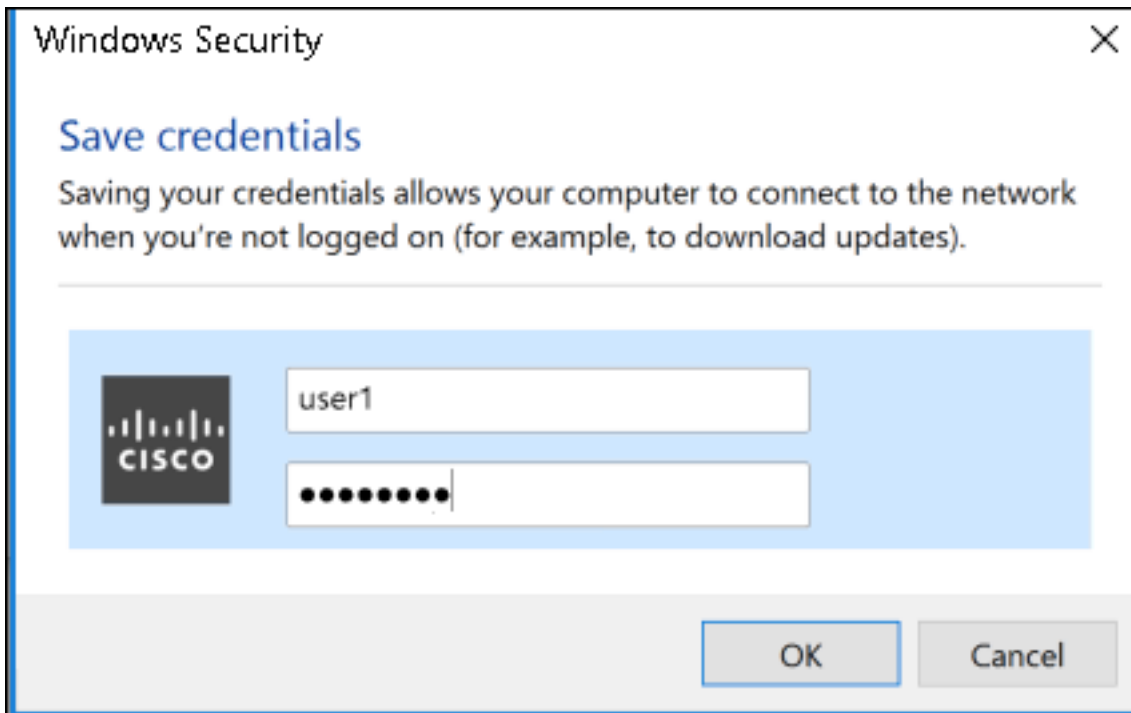
Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

OK

Cancel





## Verificar

O fluxo de autenticação pode ser verificado a partir da WLC ou da perspectiva do ISE.

### Processo de autenticação em ME

Execute este comando para monitorar o processo de autenticação de um usuário específico:

```
> debug client <mac-add-client>
```

Exemplo de uma autenticação bem-sucedida (alguma saída foi omitida):

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```

**AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client**

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48)

\*apfMsConnTask\_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

\*apfMsConnTask\_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3**

\*apfMsConnTask\_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1**

\*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth\_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x\_reauth\_sm.c:47

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Connecting state

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.342: **08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45**

.

.

.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253**

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: New PMKID: (16)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: M1 - Key Data: (22)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.979: **08:74:02:77:13:45 Starting key exchange to mobile**

08:74:02:77:13:45, data packets will be dropped

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile

08:74:02:77:13:45

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Authenticated state

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK\_START state (message 2) from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!!!

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0.....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 .....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f .....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in

PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X\_REQD (3)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP\_REQD (7) last state L2AUTHCOMPLETE (4)

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7)

pemAdvanceState2 6623, Adding TMP rule

\*Dot1x\_NW\_MsgTask\_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP\_REQD (7) Adding Fast Path rule

type = Airespace AP - Learn IP address

```

on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state
to RUN (20) last state DHCP_REQD (7)

```

Para uma maneira fácil de ler as saídas do debug client, use a ferramenta *Wireless debug analyzer*.

## [Analisador de depuração sem fio](#)

### Processo de autenticação no ISE

Navegue até **Operações > RADIUS > Logs ao vivo** para ver qual política de autenticação, política de autorização e perfil de autorização atribuídos ao usuário.

Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...			user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccess

Para obter mais informações, clique em **Detalhes** para ver um processo de autenticação mais detalhado.